APLIKASI KRIPTOGRAFI RSA MELALUI LAN MENGGUNAKAN C#.NET

Dwi Kusuma Ningrum
Jl. Dewi Sartika rt 007/06 No 42
13630
Kusumaningrum_dwi@yahoo.com

ABSTRAK

Pada penulisan skripsi ini penulis mencoba untuk membuat suatu aplikasi kriptografi dengan implementasi pada jaringan Local Area Network. Pembuatan aplikasi ini menggunakan bahasa pemrograman C#.NET. Aplikasi ini terdiri dari tiga menu yaitu menu utama sebagai tampilan awal dari program, menu kedua berupa menu untuk melakukan kriptografi sedangkan menu ketiga untuk melakukan pengkoneksian.Sehingga melalui jaringan Local Area Network dengan kelas yang sama.

Kata Kunci : Aplikasi, Cryptografi, C#.NET, Local Area Network.

PENDAHULUAN

Teknologi yang begitu pesat membuat penggunaan komputer menjadi sangat penting hal ini juga diikuti oleh berkembangnya telekomuninkasi, salah satunya internet.Melalui internet kita dapat mengenal dunia luar dengan cepat, namun internet memiliki beberapa kekurangan salah satunya adalah keamanan data sehingga menimbulkan tantangan dan tuntutan akan tersedianya suatu sistem pengamanan data yang sama canggihnya dengan kemajuan teknologi komputer itu sendiri.

Salah satu pencegahan yang daoat kita buat adalah menggunakan aplikasi bebbasiskan kriptografi. Banyak orang yang terasa asing dengan kata kriptografi, padahal kata ini sering digunakan dalam penggunaan jaringan komputer. Mungkin sudah banyak yang pernah membuat proyek seperti ini dengan alagoritma yang berbeda-beda. Namun pada aplikasi ini algoritma yang digunakan adalah RSA dengan menggunakan C#.NET yang diimplementasikan pada jaringan LAN. Apilkasi ini hanya berupa kriptografi yang digunakan pada tulisan.

TINJAUAN PUSTAKA

Penelitian ini menunjukkan bahwa kriptografi merupakan sebuah aplikasi yang dapat digunakan dalam pengamanan data. Banyak algoritma yang dapat digunakan dalam kriptografi saah satunya adalah RSA.

METODE PENELITIAN

Data yang dan dalam penelitian dapat beragam data, namun data tersebut harus berupa teks. Metode yang digunaliteratir melihat kan adalah metode literatur yaitu penulis dalam membuat program.

PEMBAHASAN

Kriptografi dalam sejarahnya tercatat dipergunakan secara terbatas oleh bangsa Mesir 4000 tahun lalu. Kriptografi (*Cryptography*) berasal dari dua kata yaitu "*Crypto & graphy*" yang dalam sudut bahasa "*Crypto*" dapat diartikan rahasia (*secret*) dan *"graphy"* dapat diartikan tulisan (*writing*) jadi Kriptografi (*Cryptography*) dapat diartikan sebagai suatu ilmu atau seni untuk mengamankan pesan agar aman dan dilakukan oleh *"Cryptographer"*. Sebuah pesan yang tidak disandikan atau dienkripsi disebut sebagai **plaintext** atau disebut juga sebagai **cleartext**. Sedangkan pesan yang telah disandikan dengan sebuah algoritma kriptografi disebut sebagai **ciphertext**.Proses untuk mengubah plaintext ke chipertext disebut **encryption** atau **encipherment**. Sedang proses mengubah chipertext ke plaintext disebut **decryption** atau **decipherment**.

Fasilitas untuk mengkonversikan sebuah plaintext ke ciphertext atau sebaliknya disebut *Cryptographic system* atau *Cryptosystem* dimana sistem tesebut terdiri dari algoritma–algorima tertentu yang tergantung pada sistem yang digunakan. Algoritma kriptografi (*cryptographic algorithm*) disebut *cipher* yang merupakan persamaan matematik yang digunakan dalam proses enkripsi dan deskripsi dimana proses tersebut diatur oleh satu atau lebih kunci kriptografi. Kunci-kunci tersebut secara umum digunakan untuk proses pengenkripsian dan pendekripsian tidak perlu identik, tergantung sistem yang digunakan.

Proses enkrisi dan deskrisi secara matematis diterangkan sebagai berikut :

EK (M) = C (Proses Enkripsi)

DK (C) = M (Proses Deskripsi)

Keterangan :

EK : Enkripsi.

DK : Deskripsi.

M : Message (Pesan sebelum dienkripsi).

C : Cipher (Pesan setelah dienkrisi).

Secara umum algoritma kriptografi diciptakan oleh orang yang berpengalaman dalam bidang keamanan data dan mungkin pernah membuka sebuah algoritma kriptografi tanpa bantuan kunci. Pelaku yang melakukan tindakan memecahkan *ciphertext* tanpa bantuan kunci disebut *Crytpanalyst*. Sedangkan Ilmu dan seni membuka (*breaking*) ciphertext tanpa bantuan kunci disebut *Cryptanalysis*.

Tujuan Kriptografi

Beberapa fungsi yang ada dari penggunaan kriptografi adalah sebagai berikut :

1. Melindungi data agar tidak dapat dibaca oleh orang-orang yang tidak berhak.
2. Mencegah agar orang-orang yang tidak berhak, menyisipkan atau mengahapus data.

Sedangkan tujuan dari sistem kriptografi adalah sebagai berikut :

1. Confidentiality

Memberikan kerahasiahan pesan dan menyimpan data dengan menyembunyikan informasi lewat teknik-teknik enkripsi.

2. Message Integrity

Memberikan jaminan untuk tiap bagian bahwa pesan tidak akan mengalami perubahan dari saat ia dibuat sampai saat ia dibuka.

3. Non-repudiation

Memberikan cara untuk membuktikan bahwa suatu dokumen datang dari seseorang apabila ia mencoba menyangkal memiliki dokumen tersebut.

4. Authentication

Memberikan dua layanan. Pertama mengidentitifikasi keaslian suatu pesan dan memberikan jaminan keontentikannya. Kedua untuk menguji identitas seseorang apabila ia akan memasuki sebuah sistem.

Kategori Kriptografi

Terdapat tiga kategori enkripsi yaitu :

1. Kunci enkripsi rahasia, dalam hal ini terdapat sebuah kunci yang digunakan untuk mengikrisi dan juga sekaligus mendeskripsikan informasi.
2. Kunci enkripsi *public*, dalam hal ini terdapat dua kunci yang digunakan, satu untuk proses enkripsi, satu lagi untuk proses deskripsi.
3. Fungsi *one-way*, dimana informasi dienkripsi untuk menciptakan "*signature*" dari informasi asli yang bisa digunakan untuk keperluan autentifikasi

Teknik Enskripsi

Dalam *Cryptosystem* menurut teknik enkripsinya dapat digolongkan menjadi dua buah, yaitu :

***Symmetric Cryptosystem* (Enkripsi Konvensional)**

Dalam *symmetric cryptosystem*,kunci yang digunakan dalam proses enkripsi dan dekripsi adalah sama atau pada prinsipnya identik. Kunci ini pun bisa diturunkan dari kunci lainnya. Oleh karena itu sistem ini sering disebut *secret-key ciphersystem*.

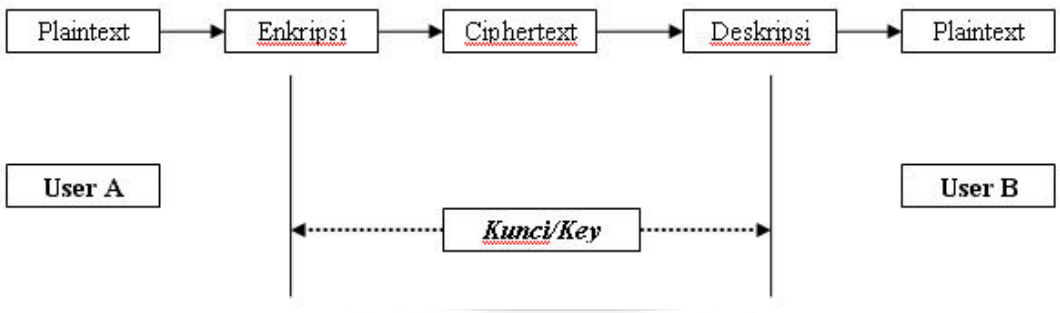
Jumlah kunci yang dibutuhkan umumnya adalah :

$$ {}_nC_2 = \frac{n.(n-1)}{2} $$

Dimana n adalah banyaknya pengguna.

Kunci yang menggunakan teknik enkripsi ini harus betul-betul dirahasiakan.

Gambaran proses enkripsi konvensional :



Gambar 1 : Konsep Kriptografi
Sumber : Dwi Kusuma Ningrum 2009

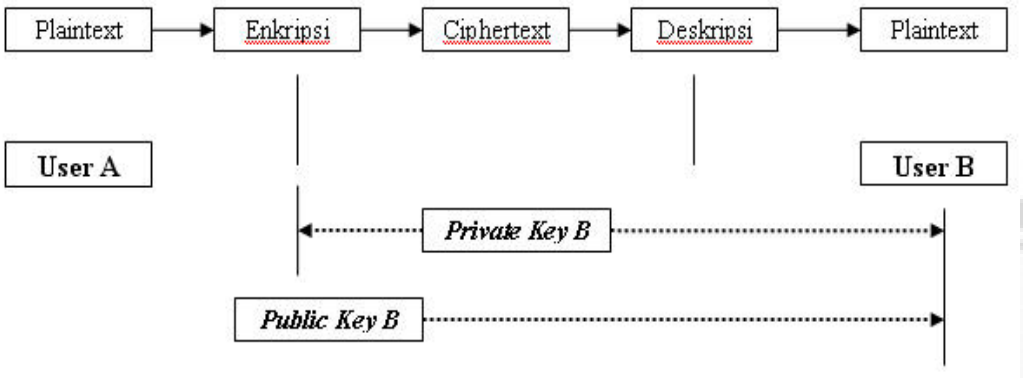
***Assymmetric Cryptosystem* (Enkripsi *public-key*)**

Dalam Assymmetric cryptosystem,kunci yang digunakan terdapat dua buah. Satu kunci yang dapat dipublikasikan deisebut kunci publik (*public key*), satu lagi kunci yang

harus dirahasiakan disebut kunci privat (*private key*). Secara sedehana proses tersebut diterangkan sebagai berikut :

- A mengirimkan pesan kepada B.
- A menyandikan pesannya dengan menggunakan kunci publik B.
- Bila B ingin membaca pesan dari A, ia harus menggunakan kunci privatnya untuk mendekripsikan pesan yang tersandikan itu.

Gambaran proses enkripsi public-key :



Gambar 2 : Kriptograf Assymetric
Sumber : Dwi Kusuma Ningrum 2009

RSA

Dari sekian banyak algoritma kunci publik yang pernah dibuat, algoritma yang paling populer adalah algoritma RSA. Algoritma RSA dibuat oleh 3 orang peneliti dari MIT\ (Massachusetts Institute of Technology) pada tahun 1976, yaitu: Ron (R)ivest, Adi (S)hamir, dan Leonard (A)dleman. Keamanan algoritma RSA terletak pada sulitnya memfaktorkan bilangan yang besar menjadi faktor-faktor prima. Pemfaktoran dilakukan untuk memperoleh kunci privat. Selama pemfaktoran bilangan besar menjadi faktor-faktor prima belum ditemukan algoritma yang mangkus, maka selama itu pula keamanan algoritma RSA tetap terjamin.

Algoritma RSA

Algoritma RSA memiliki besaran-besaran sebagai berikut:

1. p dan q, bilangan prima (rahasia)
2. n = p . q (tidak rahasia)
3. Φ(n) = (p-1)(q-1) (rahasia)

4. e (kunci enkripsi) (tidak rahasia)
5. d (kunci dekripsi) (rahasia)
6. m (plainteks) (rahasia)
7. c (chiperteks) (tidak rahasia)

Perumusan Algoritma RSA

Algoritma RSA didasarkan pada teorema Euler yang menyatakan bahwa

$$a\Phi(n) \equiv 1 \pmod{n} \quad (1)$$

dengan syarat:

1. a harus relatif prima terhadap n
2. $\Phi(n) = n(1 - 1/p1)(1 - 1/p2)\ldots(1 - 1/pr)$, yang dalam hal ini p1, p2, p3,…,pr adalah faktor prima dari n.$\Phi(n)$ adalah fungsi yang menentukan berapa banyak dari bilangan-bilangan 1, 2, 3, …, n yang relatif prima terhadap n.

Berdasarkan sifat $a^k \equiv b^k \pmod{n}$ untuk k nilangan bulat ≥ 1, maka persamaan (1) di atas dapat ditulis menjadi

$$a^{k\Phi(n)} \equiv 1^k \pmod{n} \quad (2)$$

atau

$$a^{k\Phi(n)} \equiv 1 \pmod{n} \quad (3)$$

Bila a diganti dengan m, maka persamaan (3) dapat ditulis menjadi

$$m^{k\Phi(n)}) \equiv 1^k \pmod{n} \quad (4)$$

Berdasarkan sifat $ac \equiv bc \pmod{n}$ maka bila persamaan (4) dikalikan dengan m menjadi

$$m^{k\Phi(n)+1} \equiv m \pmod{n} \quad (5)$$

yang dalam hal ini relatif prima terhadap n. Misalkan e dan d dipilih sedemikian sehingga

$$e \cdot d \equiv 1 \pmod{\Phi(n)} \quad (6)$$

atau

$$e \cdot d \equiv k\Phi(n) + 1 \quad (7)$$

Sulihkan persamaan (7) ke dalam persamaan (5) menjadi

$$m^{e \cdot d} \equiv m \pmod{n} \quad (8)$$

Persamaan (8) dapat ditulis kembali menjadi

$$(m^e)^d \equiv m \pmod{n} \quad (9)$$

yang artinya, perpangkatan m dengan e diikuti dengan perpangkatan dengan d menghasilkan kembali m semula. Berdasarkan persamaan (9), maka enkripsi dan dekripsi dirumuskan sebagai berikut:

$$E_e(m) \equiv c \equiv m^e \bmod n \quad (10)$$

$$D_d(c) \equiv m \equiv c^d \bmod n \quad (11)$$

Karena e . d = d . e, maka enkripsi diikuti dengan dekripsi ekivalen dengan dekripsi diikuti enkripsi:

$$D_d(E_e(m)) = E_e(D_d(m)) = m^d \bmod n \quad (12)$$

Oleh karena md mod n ≡ (m + jn)d mod n untuk sembarang bilangan bulat j, maka tiap plainteks m, m +n, m + 2n, …, menghasilkan cipher yang sama. Dengan kata lain, transformasinya dari banyak ke satu. Agar transformasinya satu ke satu, maka m harus dibatasi dalam himpunan {0, 1, 2, …, n-1} sehingga enkripsi dan dekripsi tetap benar seperti dalam persamaan (10) dan (11).

Algoritma Membangkitkan Pasangan Kunci

Algoritma Membangkitkan Pasangan Kunci

1. Pilih dua buah bilangan prima sembarang, p dan q.
2. Hitung n = p . q (sebaiknya p ≠ q,sebab jika p = q maka n = p2 sehingga p dapat diperoleh dengan menarik akar pangkat dua dari n).
3. Hitung Φ(n) = (p-1)(q-1).
4. Pilih kunci publik, e, yang relatif prima terhadap Φ(n).
5. Bangkitkan kunci privat dengan menggunakan persamaan (6), yaitu e .d ≡ 1 (mod Φ(n)).

Perhatikan bahwa e . d ≡ 1 (mod Φ(n)) ekivalen dengan e . d = 1 + kΦ(n), sehingga secara sederhana d dapat dihitung dengan

$$d = \frac{1 + k\Phi(n)}{e} \quad (13)$$

Hasil dari algoritma di atas adalah:

1. Kunci publik adalah pasangan (e,n)
2. Kunci privat adalah pasangan (d,n) N tidak bersifat rahasia, sebab ia diperlukan pada perhitungan enkripsi/dekripsi.

2.6.4 Algoritma Enkripsi/Dekripsi

Enkripsi:

1. Ambil kunci publik penerima pesan, e, dan modulus n.
2. Nyatakan plainteks m menjadi blokblok m1, m2, …, sedemikian sehingga setiap blok merepresentasikan nilai di dalam selang [0, n-1].
3. Setiap blok mi dienkripsi menjadi blok ci denagn rumus ci = mi e mod n.

Dekripsi:

1. Setiap blok chiperteks ci didekripsi kembali menjadi blok mi dengan rumus mi = ci d mod n.

Local Area Network

LAN pada mulanya dikembangkan oleh Universitas Hawai, dan digunakan untuk komunikasi antar pulau di Kepulauan Hawai. Pada saat itu, yang digunakan sebagai media adalah udara, dengan kata lain nirkabel. Kemudian, media udara tersebut diganti dengan kabel, dan jadilah LAN yang ada sekarang ini.

LAN diperkenalkan secara komersial pertama kali pada tahun 1980 oleh perusahaan Amerika Zerox, yang kemudian bergabung dengan Intel. Untuk kemudahan pemakaian, ditetapkan standar-standar untuk LAN, antara lain protokol-protokol. Untuk menyesuaikan dengan standar Network, pembagian layer pada LAN disejajarkan dengan tingkat fisik dan tingkat datalink. Terlebih lagi, tingkatan datalink dibagi ke dalam sub-tingkatan MAC(media access control) dan LLC(logical link control).

Pengertian dan Prinsip Kerja Local Area Network

Local Area Network (LAN),adalah jaringan yang dibatasi oleh area yang relatif kecil, umumnya dibatasi oleh area lingkungan, seperti sebuah kantor pada sebuah gedung, atau tiap-tiap ruangan pada sebuah sekolah. Biasanya jarak antar node tidak lebih jauh dari sekitar 200m.

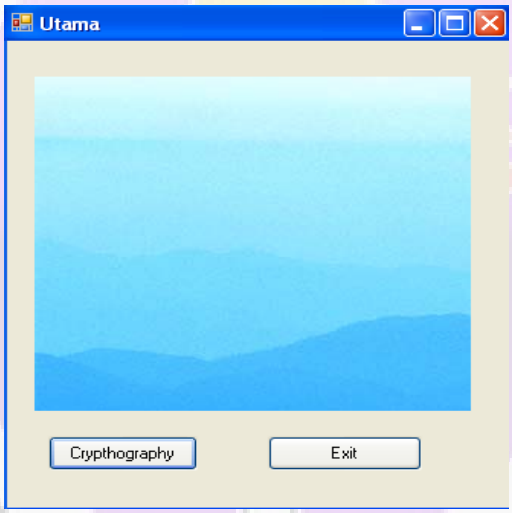
LAN dapat definisikan sebagai network atau jaringan sejumlah sistem komputer yang lokasinya terbatas didalam satu gedung, satu kompleksgedung atau suatu kampus dan tidak menggunakan media fasilitas komunikasi umum seperti telepon, melainkan pemilik dan pengelola media komunikasinya adalah pemilik LAN itu sendiri. Dari definisi diatas dapat kita ketahui bahwa sebuah LAN dibatasi oleh lokasi

secara fisik. Adapun penggunaan LAN itu sendiri mengakibatkansemua komputer yang terhubung dalam jaringan dapat bertukar data atau dengan kata lain berhubungan. Kerjasama ini semakin berkembang dari hanya pertukaran data hingga penggunaan peralatan secara bersama. LAN yang umumnya menggunakan hub, akan mengikuti prinsip kerja hub itu sendiri. Dalam hal ini adalah bahwa hub tidak memiliki pengetahuantentang alamat tujuan sehingga penyampaian data secara broadcast, dan juga karena hub hanya memiliki satu domain collision sehingga bila salah satu port sibuk maka port-port yang lain harus menunggu.

HASIL

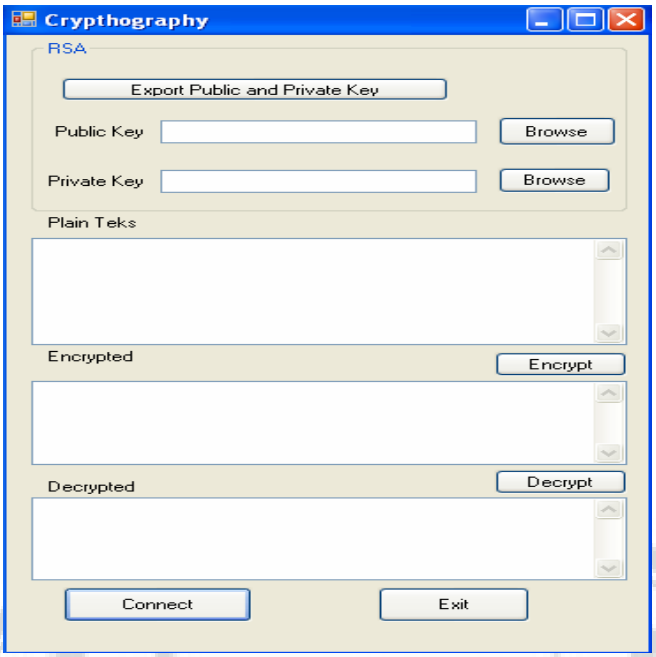
Hasil dari aplikasi ini dapat dilihat berikut ini :

1. Pembukaan dari program seperti di bawah ini :



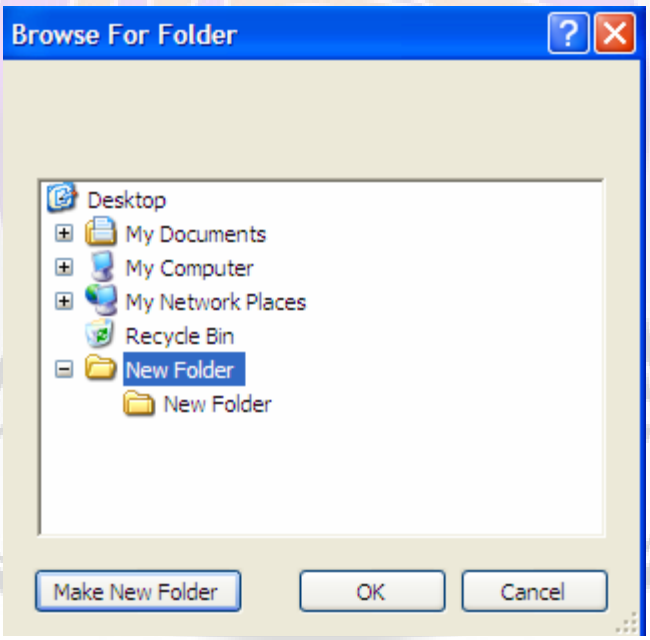
Gambar 3 : Tampilan Form Utama
Sumber : Dwi Kusuma Ningrum 2009

2. Setelah itu pilihlah button Cryptography kemudian muncul Form seperti si bawah ini :

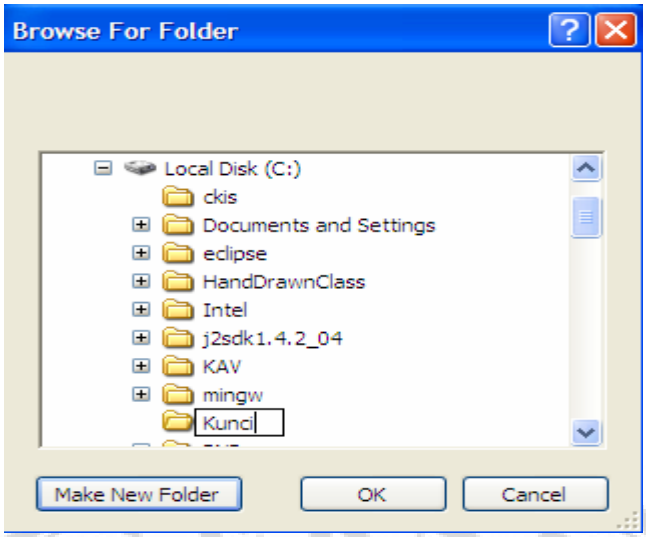


Gambar 4 : Tampilan Form Crypthography
Sumber : Dwi Kusuma Ningrum 2009

3. Memilih button export public and private key ini dimaksudkan agar kiata memiliki key untuk private dan public key

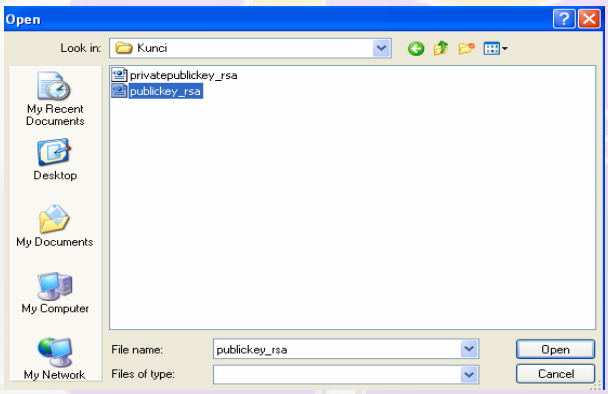


Gambar 5 : Tampilan Jika memilih Export Public and Private key
Sumber : Dwi Kusuma Ningrum 2009



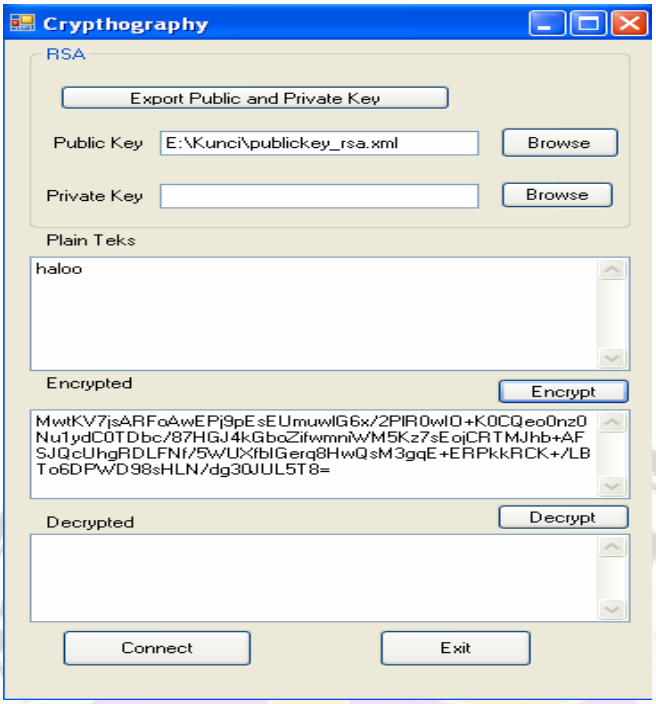
Gambar 6 : Tampilan memilih Make New Folder
Sumber : Dwi Kusuma Ningrum 2009

4. memilih button browse untuk public key, kemudian cari pubilc key yang digunakan



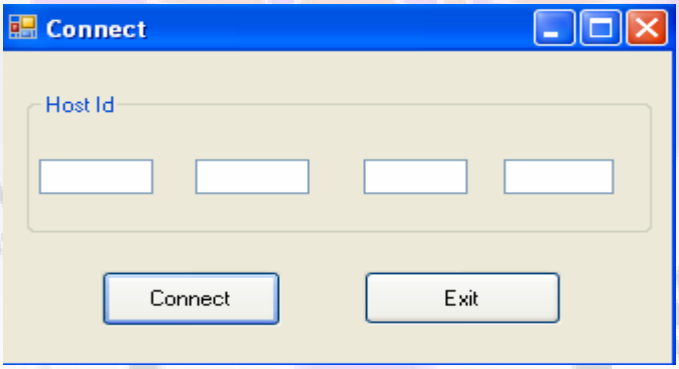
Gambar 7 : Tampilan Mengambil Public Key
Sumber : Dwi Kusuma Ningrum 2009

5. isilah plain teksnya
6. klik button encryption

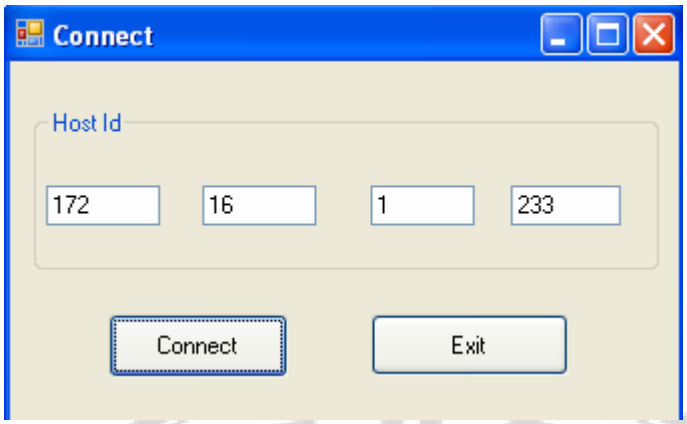


Gambar 8 : Tampilan Form Crypthography Dijalankan
Sumber : Dwi Kusuma Ningrum 2009

7. pilih connect ntuk mengkoneksi
8. masukkan ip addressnya

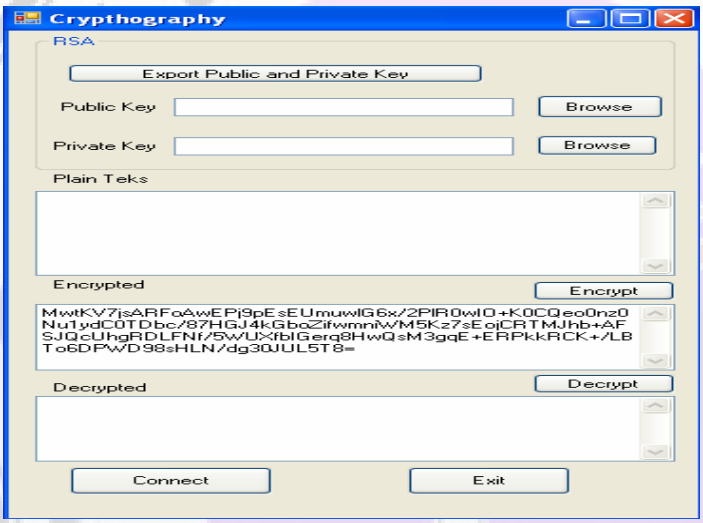


Gambar 9 : Tampilan Form Connect
Sumber : Dwi Kusuma Ningrum 2009

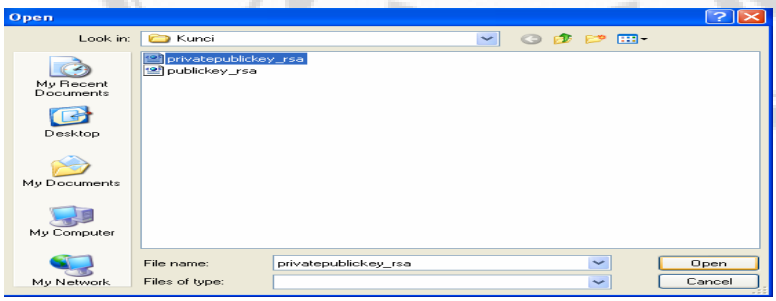


Gambar 10 : Tampilan Form Connect saat dijalankan
Sumber : Dwi Kusuma Ningrum 2009

9. kembali ke form kriptografi untuk mengembalikan teksnya

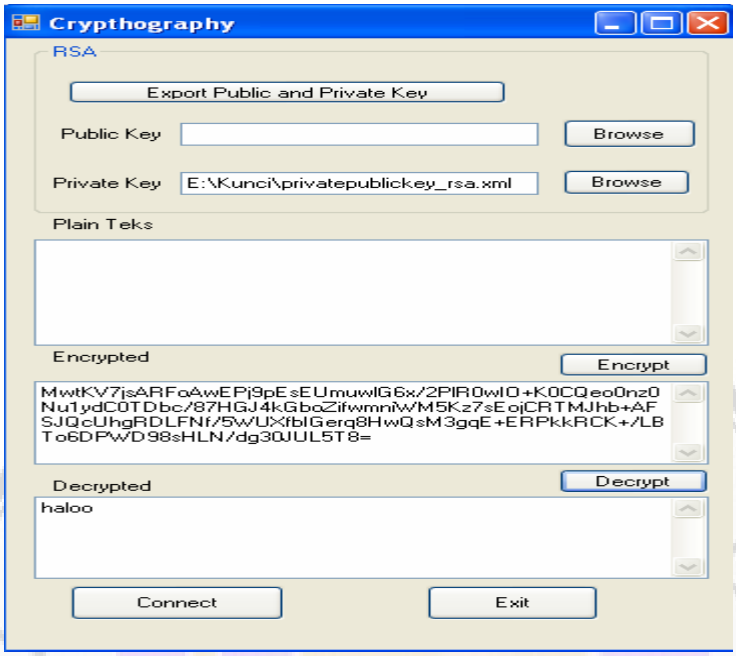


Gambar 11 : Tampilan Form Crypthography saat dipilih dari form connect
Sumber : Dwi Kusuma Ningrum 2009
10. ambil private key dengan menekan button browse



Gambar 12 : Tampilan mengambil Private Key
Sumber : Dwi Kusuma Ningrum 2009

11. klik Decrypt untuk mengembalikan teks



Gambar 13 : Tampilan Form Crypthography saat di deskripsi
Sumber : Dwi Kusuma Ningrum 2009

KESIMPULAN

Aplikasi kriptografi merupakan hal yang baru dikenal oleh sebagian orang, namun bagi orang yang bekerja pada bagian keamana data hal ini bukanlah suatu hal yang asing lagi pada zaman sekarang ini, apalagi didukung dengan tekhnologi yang berkembang semakin pesat khususnya di bidang teknologi informatika. Banyak jenis kriptografi yang dapat digunakan dalam pembuatan kriptografi, seperti kriptografi DES, Blowfish, MD5, RSA dan lainnya yang dapat dibuat dengan menggunakan berbagai macam jenis bahasa pemrogrman yang ada.

Dengan menggunakan bahasa pemrograman C#.NET, penulis membuat suatu Aplikasi kriptografi. Aplikasi ini merupakan aplikasi sederhana yang dibuat untuk membuat kriptografi lebih mudah digunakan. Kriptografi yang dgunakan adalah kriptografi RSA dengan menggunakan sepasang kunci sehingga keamanan data lebih terjamin,selain itu aplikasi ini dapat digunakan untuk pengiriman data melalui jaringan LAN.

Penulis memilih bahasa pemrograman C#.NET karena memiliki fasilitas-fasilitas yang mendukung dan mempermudah dalam pembuatan aplikasi tersebut. Hal ini tidak terlepas juga dengan referensi yang didapat oleh penulis. Selain itu spesifikasi komputer yang dibutuhkan untuk instalasi bahasa ini tidaklah terlalu besar. Oleh karena itu penulis menggunakan bahasa pemrograman C#.NET.

Saran

Program yang terdapat dalam aplikasi ini masih sederhana dan masih terdapat banyak kekurangan, terutama dalam hal enskripsi dan deskripsi data. Dalam pengembangan selanjutnya, program ini memungkinkan untuk pembuatan aplikasi yang lebih lengkap lagi dari yang penulis buat. Oleh karena itu saran dari semua pihak sangat penulis harapkan untuk memperbaiki ataupun mengembangkan aplikasi ini lebih lanjut.

DAFTAR PUSTAKA

Rinaldi Munir, *Kriptografi*, Informatika, Jakarta, 20 Oktober 2006

Anonim, *Crypthography.html*, http://www.wikipedia.com, Indonesia, 8 Agustus 2008

Anonim, *Kriptografi.html,* http://www.google.com, Indonesia, 20 Agustus 2008

Anonim, *socket_TCP/IP.html*, http://www.google.com, Indonesia, 30 Agustus 2007

Anonim, *Kriptografi Kunci Public.pdf*, http://www.google.com, Indonesia, 2 September 2008

Anonim, *Sejarah LAN.doc* ://www.google.com, Indonesia, 2 Desember 2008

Anonim, *IP Adress.html*://www.wikipedia.com, Indonesia, 2 Desember 2008